Memoria Final TFM

Aspectos Legales

Junio de 2012

Fabian Andres Medina Becerra
Estudiante MISTIC

Universitat Oberta de Catalunya

Contenido

Análisis Caso 1 2
Antecedentes de hechos 3
Fundamentos de derecho 3
Análisis Caso 2 6
Antecedentes de hechos 6
Fundamentos de derecho 7
Análisis Caso 3 9
Antecedentes de hechos 10
Fundamentos de derecho 11

Análisis Caso 1

El Hospital General de Gerona acaba de implantar el programa GEPLATEC.

Gerona, plataforma tecnológica (GEPLATEC), es un plan piloto de informatización clínica pionero en Europa en la utilización de las nuevas tecnologías al servicio de la sanidad pública.

Este proyecto se concreta en la digitalización de las imágenes radiológicas y la redacción de la historia clínica del paciente directamente en soporte informático (Historia Clínica Electrónica). De esta manera, desde cualquier servicio del hospital y -lo que es más novedoso- desde cualquier centro de salud de la ciudad, se puede consultar esta documentación, con lo que aumenta el tiempo de consulta efectiva.

Además, se han creado las estaciones clínicas de trabajo, esto es, un terminal situado a pie de cama del paciente que permite al médico y enfermero visualizar los diferentes episodios clínicos del enfermo y gestionar las órdenes y los planes de cuidado, pudiendo, incluso, emitir el informe de alta clínica. Los resultados de las pruebas diagnósticas también se registrarían desde el lugar de origen. Con todo ello se agiliza la recepción de estos resultados y se ahorra una gran cantidad de papel, lo que convierte a esta área de salud en una de las más ecológicas de España.

El Hospital General de Gerona es ahora uno de los pocos centros europeos en donde se han producido simultáneamente la generalización de estaciones clínicas de trabajo y la digitalización de imágenes radiológicas.

La eliminación de las tradicionales placas, contribuye a que el Hospital de Gerona se convierta en un centro más ecológico y que los enfermos sean menos expuestos a estas pruebas diagnósticas. La disponibilidad de la información es uno de los aspectos más relevantes de este programa, pues ha permitido que la historia clínica de un paciente pueda ser accesible inmediatamente en todas las zonas de la instalación sanitaria.

Por otra parte, el citado hospital –junto con otros cinco hospitales catalanes—ha accedido a una petición del Consorcio para la Normalización Lingüística de la Generalitat, facilitando 846 historias clínicas a la empresa privada Centro Informático de Estadísticas y Sondeos, a fin de controlar el empleo del catalán en dichas historias y elaborar un estudio estadístico sobre el uso de aquel idioma y del castellano en los centros sanitarios de Cataluña. En concreto, 282 corresponden a “hospitalización”, 282 a “consultas externas” y 282 a “urgencias”.

En virtud de lo anterior, los encuestadores tendrán acceso a los datos identificativos de los pacientes en dichos hospitales, aunque el uso que se hará del análisis documental afectará exclusivamente a la lengua de los documentos y no del contenido.

En dicha operación, no se ha recabado el consentimiento de los enfermos cuyos expedientes fueron cedidos, pero el Hospital de Gerona ha suscrito un compromiso de confidencialidad con la empresa privada CIES, en el que explícitamente se exige que los datos que obtengan sólo se utilicen para el objetivo del estudio.

Antecedentes de hechos

PRIMERO. El Hospital General de Girona, ha accedido a una petición del Consorcio para la Normalización Lingüística de la Generalitat, con el fin de facilitar 846 historias clínicas a la empresa privada Centro Informático de Estadísticas y Sondeos, a fin de controlar el empleo del catalán en dichas historias y elaborar un estudio estadístico sobre el uso de aquel idioma y del castellano en los centros sanitarios de Cataluña. Del total de las 846 historias clínicas, 282 corresponden a "hospitalización", 282 a "consultas externas" y 282 a "urgencias".

SEGUNDO. Los encuestadores, pertenecientes al Centro Informático de Estadísticas y Sondeos, tuvieron acceso a los datos identificativos de los pacientes en dichos hospitales, aunque, aclara, el Consorcio, el uso del análisis documental afectará exclusivamente a la lengua de los documentos y no del contenido.

TERCERO. En dicha operación, no se ha recabado el consentimiento de los enfermos cuyos expedientes fueron cedidos, pero el Hospital de Gerona ha suscrito un compromiso de confidencialidad con la empresa privada CIES, en el que explícitamente se exige que los datos que obtengan sólo se utilicen para el objetivo del estudio.

Fundamentos de derecho

I
Es válida la aplicación del procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalitat, previsto en el Decreto 278 de 1993, el artículo 17 de la Ley 5 de 2002 de la Agencia Catalana de Protección de Datos, además del título VII de la LOPD.

II
El Hospital General de Girona es la entidad responsable de los ficheros de historias clínicas, de acuerdo a lo dispuesto en el Decreto 29 de 10 de enero de 1995, por el que se regulan los ficheros automatizados que contienen datos de carácter personal en el ámbito del Departamento de Sanidad y seguridad Social. Adicionalmente en lo dispuesto en la LOPD, en lo referente a responsable del fichero.

Por lo tanto, sin importar que el estudio fuera liderado por un organismo perteneciente a la administración pública, el responsable de garantizar que los datos se trataran de conformidad a la LOPD es el responsable del fichero.

El literal d del artículo 3 de la LOPD define:
"Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

III
Ahora bien, una vez determinado el responsable del fichero, se debe determinar si existía autorización que permita el acceso por parte de los realizadores del estudio, en este caso el Centro Informático de Estadísticas y Sondeos, a los datos contenidos en las historia clínicas del Hospital General de Girona.

Es necesario por tanto recurrir a lo descrito en la LOPD, la cual contiene indicaciones específicas al tratamiento de datos personales, entre otros y especialmente los referentes a salud.

El numeral 1 del artículo 4 de la LOPD dispone:
"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

El acceso a información médica puede ser excesivo, máxime cuando el objetivo del estudio es la utilización del catalán, y por tanto contraria al principio de calidad de los datos consignada en el anterior artículo. Entonces pues, era posible fragmentar la información disponible de los pacientes a fin de apartar los datos relativos a la salud y sin embargo cumplir con el objetivo del estudio.

El numeral 3 del artículo 7 de la LOPD establece:
"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".

Así mismo el numeral 6 del artículo 7 de la LOPD establece:
"No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto."

La LOPD es muy específica en los requerimientos exigidos al tratamiento de datos referentes a salud. Debe existir una ley que así lo disponga o su consentimiento expreso (el del afectado) o es necesario para la utilización de servicios médicos sanitarios. Pero ninguna de estas salvedades es el origen del tratamiento que hiciera el Hospital General de Girona junto con el Centro Informático de Estadísticas y Sondeos.

Adicionalmente la Ley 21 de 29 de diciembre de 2000, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica, en su artículo 11 da cuentas de los usos que se le pudieran dar a una historia clínica.

El primer uso dispuesto es el de garantizar la asistencia adecuada del paciente, esto dirigido a las funciones propias de los profesionales de la salud.

En el numeral 3 del mismo artículo se establece el acceso a las historias con fines de investigación, epidemiológicas, de investigación o docencia, pero obliga a "preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, excepto que el paciente haya dado antes su consentimiento".

Por lo anterior se dispone de dos formas de acceso a los datos: sin la identificación de los pacientes o mediante su consentimiento previo.

Para el caso en cuestión, es decir, un estudio de uso de un idioma, no es una regla de excepción para el acceso a los datos y si así fuera se hubiese debido utilizar alguna de las dos formas de acceso antes mencionadas.

Por último y no menos importante, es posible acceder a esta información (historias clínicas), para la realización de estadísticas, de acuerdo a lo dispuesto en el literal b, numeral 3 del artículo 2 de la LOPD "Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública".

Y de esta misma manera, la Ley 23 de 30 de diciembre de 1998 de estadística de Cataluña establece que:

"La información que se solicite para elaborar estadísticas de interés de la Generalidad se satisfará de manera completa y verídica, dentro de los plazos establecidos, respetando los formatos y las indicaciones que se establezcan sobre el soporte de la información, y garantizará la protección de los datos personales en el marco de la legislación vigente".

Por lo anterior se implica que solamente es aplicable a información recabada para la realización de estadísticas oficiales.

En resumen, ninguna de las legislaciones anteriormente expuestas (derechos de información relativos a la salud, estadísticas, protección de datos), admiten el acceso a los datos contenidos en las historias clínicas, tal como en el hecho ocurrido. Esto es, el responsable del fichero y su tratamiento, el Hospital General de Girona, no contaba con la autorización para que terceros tuviesen acceso a las historias clínicas de sus pacientes, lo cual se convierte en una vulneración al derecho fundamental de la protección de datos.

IV

El literal d, numeral 3 del artículo 44 de la LOPD establece que:
"La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.".

Y el artículo 10 de la LOPD indica:
"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal estén obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

Por todo lo anterior se concluye que el Hospital General de Girona, responsable de las historias clínicas de sus pacientes vulneró el deber del secreto establecido en el artículo 10 de la LOPD, por tanto ha cometido una infracción grave, contenida en el d, numeral 3 del artículo 44 de la LOPD, ya que ha compartido datos personales y referentes a salud de sus pacientes, permitiendo el acceso de terceros a tales datos, sin presentarlos de forma anónima ni sin su consentimiento y sin que exista ley alguna que lo obligue.

El artículo 10 de la LOPD hace al responsable del fichero, encargado de guardar el secreto profesional respecto de los datos personales objeto de tratamiento, con el fin de evitar que los mismos sean tratados por personal no autorizado.

Análisis Caso 2

Por otra parte, según se ha publicado recientemente en diversos medios de comunicación, 3.000 historias clínicas del Hospital General de Gerona se han filtrado en Internet a través de eMule. La Unidad de Delitos Tecnológicos de los Mossos d'Esquadra fue la que encontró las historias clínicas en eMule. Una vez conocido el problema, la Agencia de Protección de Datos ha abierto una inspección y se ha comprobado que el centro médico (HGG) tiene un fichero de gestión de pacientes igual al que se ha hallado en Internet. Ese fichero contiene datos de pacientes tratados en distintos departamentos (ginecología, anatomía patológica, etc.).

Según se ha publicado, se desconoce la causa de dicha filtración aunque la hipótesis que cobra mayor fuerza es que el desconocimiento técnico de un empleado del Hospital hizo que pusiera a disposición del programa eMule todos esos datos, contenidos en una carpeta del disco duro de su ordenador.

Antecedentes de hechos

PRIMERO. Se tiene conocimiento que la Unidad de Delitos Tecnológicos de los Mossos d'Esquadra, encontró un archivo de base de datos, a través de un usuario del programa de compartición eMule. Una vez verificado el contenido del archivo, se comprueba que corresponden a historias clínicas del centro sanitario Hospital General de Gerona.

SEGUNDO. La Agencia Española de Protección de Datos abrió una inspección y se comprobó que el centro médico Hospital General de Gerona, tiene un fichero de gestión de pacientes igual al que se ha hallado en internet.

TECERO. La Agencia Española de Protección de Datos consideró que los anteriores hechos hacen referencia a ficheros de datos de carácter personal, responsabilidad el Hospital general de Gerona, incluidos en el ámbito de aplicación del artículo 7 de la Ley Orgánica de Protección de Datos Personales de 1999.

CUARTO. Se especula que la causa de dicha filtración sea el desconocimiento técnico de un empleado del Hospital, quien por ignorancia podría haber incluido tal información en una compartida que utiliza el programa eMule.

QUINTO. Se hace necesario abrir una investigación al Hospital General de Gerona, por la presunta violación de los artículos 9 y 10 de la Ley Orgánica de Protección de Datos Personales de 1999. Las anteriores conductas son tipificadas como graves, en el artículo 44.3 de la LOPD.

SEXTO. A continuación desglosan las infracciones en las que ha incurrido el Hospital:

1. Vulneración del artículo 10 de la LOPD, tipificada como una conducta muy grave en el artículo 44, numeral 3, literal d, "La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley".

2. Vulneración del artículo 9 de la LOPD, tipificada como una conducta grave en el artículo 44, numeral 3, literal h, "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

Fundamentos de derecho

I

Es competencia del Director de la Agencia de Protección de Datos resolver el procedimiento, tal como se dispone en el artículo 41, numeral 1 y artículo 46 de la LOPD. Tal procedimiento se ajustará a lo previsto en el Título IX del Real Decreto 1720 de 2007, Procedimientos Tramitados por la Agencia Española de Protección de Datos.

II

De acuerdo a lo dispuesto en el artículo 9 de la LOPD, en el cual se indican los principios de seguridad de la información contenidos en los ficheros, da cuenta de las medidas de seguridad técnicas y organizativas a tener en cuenta por los encargados del tratamiento, en lo que se refiere a salvaguardar la confidencialidad, la integridad y la disponibilidad de los datos.

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

Ahora bien, es importante tener en cuenta que para el caso en cuestión, se observe detenidamente si es aplicable lo relacionado anteriormente, correspondiente al artículo 9 de LOPD. En primer lugar se debe remitir a las definiciones de "responsable del fichero", "fichero" y "tratamiento".

El artículo 3, literal b, define fichero como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento,

organización y acceso", independiente del medio en el que se encuentre. El literal d, indica que el responsable del fichero o tratamiento es la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento", que, para este caso corresponde al Hospital, pues es el responsable del contenido y uso de la información contenida en el fichero. Así mismo, en el literal c, ser refiere al tratamiento como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias", esto es, todo aquel proceso que se realice con los ficheros.

Adicionalmente, el artículo 81, numeral 3 del Real Decreto 1720 de 2007, establece que las medidas de seguridad para información que se refiera a la salud, deberán ser de nivel básico, medio y alto. Este tipo de medidas deberían ser las aplicables por parte del Hospital, debido al tipo de información inherente de que trata el fichero. Por lo tanto, serían aplicables las medidas de seguridad aplicables a los ficheros y tratamientos automatizados, esto por estar contenido en medio digital, contenidas en el Capítulo III del RD 1720. Estas medidas se encuentran descritas desde al artículo 89 hasta el artículo 104, en los que se describen las medidas de seguridad de nivel básico, medio y alto. Además de las medidas básicas y medias, es necesario tener en cuenta:

1. La gestión y distribución de soportes.
2. Copias de respaldo y distribución.
3. Registro de accesos

En búsqueda realizada a través de internet, no se encontró información acerca de reglamentación especial para la Comunidad de Cataluña.

Por último, y no menos importante es de considerar lo concerniente al acceso a los datos por cuenta de terceros, enmarcado dentro del artículo 12 de LOPD. El numeral dos de este artículo indica que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".

A la luz de este artículo, el Hospital General de Gerona está obligado a implementar las medidas de seguridad suficientes para que terceros no autorizados no tengan acceso a la información de sus pacientes. Sin embargo, el Hospital no adoptó los controles necesarios para que un miembro de su personal médico o administrativo, primero, instalara software de compartición de archivos y segundo manipulara el archivo de tal forma que lo llevara a la carpeta compartida de dicho software.

A la luz de los hechos, el Hospital es responsable de los datos y por tanto, debe adoptar, como mínimo, las medidas estipuladas en la legislación del tema, con el fin que no se presenten nuevamente casos, en los cuales se incorpore información a equipos no autorizados, sean del Hospital o personales y se logra acceso de terceros.

III
El artículo 44, numeral 3, literal d, de LOPD, considera infracción grave:
"La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley".

En este caso, se comprueba que los datos que se expusieron en internet, a través del programa eMule, se consideran datos especialmente protegidos en el artículo 7 de LOPD. Al igual que los datos relativos a la salud, los datos de origen racial y vida sexual, entre otros, deben ser tratados como datos sensibles. Por lo tanto se exige a aquellos organismos encargados de su tratamiento, la debida diligencia con el fin de asegurar que se cumpla con la normatividad exigida por LOPD.

En lo que se refiere al deber de secreto, LOPD en su artículo 10 indica:
"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal estén obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

Este artículo hace referencia a una de las características que propende la seguridad de la información, la confidencialidad.

De la confidencialidad no solamente es responsabilidad del responsable del archivo, sino también quienes intervienen en su tratamiento. Este deber no solamente es obligatorio durante la relación laboral, sino, también después de finalizar la relación.

Para el caso en cuestión, cualquier usuario del programa eMule, conectado a internet, podía acceder al fichero expuesto en la carpeta compartida de dicho software, la cual se encontraba en un equipo del Hospital. Por lo tanto, el Hospital, siendo responsable de los datos, vulnero este principio, al no contar con los controles que evitaran el acceso no autorizado.

IV
El artículo 44, numeral 3, literal h, de LOPD, considera igualmente una infracción grave:
"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

Este caso se considera una violación del "principio de seguridad de los datos", estipulado en el artículo 9 de LOPD y considerada grave en el anterior artículo.

Análisis Caso 3

Posteriormente, unos 6 meses después de lo anterior, durante los meses de enero y febrero de 2009, la empresa llevó a cabo una auditoria informática para revisar la seguridad del sistema y detectar las posibles anomalías de utilización de los medios puestos a disposición de los empleados, constatando que uno de ellos, el Sr. Óscar E., durante el período reseñado y en horas de trabajo, utilizó los accesos a Internet desde su terminal y con su clave para navegar y acceder a

páginas ajenas a su trabajo y en número altamente desproporcionado por desmedido, hasta un total de 4669 accesos de uso o interés particular, del total de 5556 páginas visitadas.

El Sr. Oscar M. había prestado servicios como empleado en la empresa desde el 22/01/1992 hasta su despido disciplinario por falta muy grave, que tuvo lugar en fecha 13/03/2009. Dicho despido fue notificado al denunciante mediante escrito de la misma fecha, en el que se detallan los hechos que determinaron el acuerdo de la entidad empleadora.

A la carta de despido se acompañaron las 66 páginas del "Reporte de Auditoria Detallada del Utilizador", que muestra un estudio de las páginas visitadas y su categorización (motores de búsqueda, música, juegos, financiero, salud y medicina, redes sociales, etc…), así como un listado de las direcciones visitadas, fecha y hora de acceso.

Debe tenerse en cuenta que la empresa no había definido una política de uso de las nuevas tecnologías puestas a disposición de los trabajadores ni había informado a los trabajadores de que se instauraría un control así como de los medios que se aplicarían en orden a comprobar la corrección del uso de los medios informáticos.

Antecedentes de hechos

PRIMERO. La empresa XXX, llevó a cabo entre los meses de enero y febrero de 2009, una auditoría informática para revisar la seguridad del sistema y detectar las posibles anomalías de utilización de los medios puestos a disposición de los empleados.

SEGUNDO. De acuerdo a un informe de auditoría informática, se detectaron posibles anomalías de utilización, en un ordenador puesto a disposición del Sr. Oscar, mediante el acceso a internet a páginas ajenas a su trabajo y en número altamente desproporcionado. El informe indica que de un total de 5556 páginas visitadas, 4669 fueron accesos a páginas de interés particular, en el periodo de realización de la auditoría y en horas laborales.

TERCERO. La empresa dio por terminado el contrato laboral con el Señor Oscar, quien laboró desde el 22 de enero de 1992 hasta el 13 de marzo de 2009, soportando tal despido en el "Reporte de Auditoría Detallada del Utilizador", en el cual se muestra un estudio de las páginas visitadas y su categorización (motores de búsqueda, música, juegos, financiero, salud y medicina, redes sociales, etc…), así como un listado de las direcciones visitadas, fecha y hora de acceso.

CUARTO. La empresa XXX, no ha definido una política de uso de las nuevas tecnologías puestas a disposición de los trabajadores, ni ha informado a los trabajadores que se instauraría un control así como de los medios que se aplicarían en orden a comprobar la corrección del uso de los medios informáticos.

QUINTO. El ahora ex trabajador, Señor Oscar, impugna su despido, aduciendo una infracción al artículo 18 de la Ley del Estatuto de los Trabajadores, al numeral 1 del artículo 90 de la Ley de Procedimiento Laboral y al numeral 1 del artículo 18 de la Constitución Española.

Fundamentos de derecho

I

De acuerdo a lo dispuesto en el artículo 18 de la Ley del Estatuto de los Trabajadores, en el cual se indican los requisitos que debe cumplir una empresa al momento de realizar un registro sobre las pertenencias de un trabajador.

"Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible".

En este punto es importante analizar si las condiciones que este artículo establece para el registro de la persona del trabajador, su taquilla y efectos particulares, se aplican también al ordenador facilitado al trabajador para el cumplimiento de sus funciones.

En primer lugar se debe tener en cuenta que este medio (el ordenador), es propiedad de la empresa y por tanto se considera dentro del ámbito de poder de vigilancia del empresario. Cosa contraria con lo que sucede con un casillero, por ejemplo, en el que el casillero es propiedad de la empresa pero las pertenecías que allí se encuentran son del trabajador y no hacen parte de los medios que facilita el empresario para el desarrollo de sus actividades.

En segundo lugar, existirá la posibilidad de una utilización personal, no solamente la ligada al ejercicio de sus funciones. Está posibilidad se presenta debido a la dificultad de establecer una prohibición absoluta del uso personal del ordenador. Así mismo de un uso permisivo y tolerante a la utilización moderada de estos medios para fines personales.

En tercer lugar es posible que el uso de estos medios informáticos, ordenador e internet, puedan presentarse eventos que atenten a la intimidad de los trabajadores, en este caso en lo concerniente a la navegación en internet y al acceso a ciertos archivos en el ordenador que se pueden denominar personales.

Estas consideraciones implican que el artículo 18 de la Ley de Estatuto de los Trabajadores no es aplicable al control de la empresa de los medios, en este caso el ordenador, que se facilita al trabajador para el desempeño de sus funciones.

II

El numeral 3 del artículo 20 de la Ley del Estatuto de los trabajadores, brinda indicaciones acerca de las medidas de control y vigilancia que puede utilizar un empresario a fin de verificar el cumplimiento de sus funciones.

"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".

Para el caso de análisis, se debe tener en cuenta que tanto el ordenador como el servicio de internet son propiedad del empresario, quien los facilita al trabajador para el cumplimiento de sus funciones, por lo que se deduce que su utilización se ampara dentro del ámbito de control y vigilancia del empresario, haciendo énfasis en que se debe tener en cuenta la consideración debida a su dignidad humana.

Ahora bien, es necesario establecer los límites de los controles por parte del empresario, considerando siempre la dignidad humana y el respeto a la intimidad, ésta última consagrada en el artículo 18 de la Constitución Española de 1978. Es de resaltar cierto grado de tolerancia generalizada en usos personales a medios como los del objeto de este análisis. Esta tolerancia se debe tratar con mucho cuidado, no llegando al extremo en el que el trabajador imponga el respeto al derecho a la intimidad, pues está haciendo uso de medios proporcionados por la empresa, ni al extremo de convertirse en un impedimento para realizar el control empresarial.

Para que situaciones como estas puedan ser dirimidas convenientemente, tanto a favor del trabajador, como del empresario, es necesario que desde el momento de la vinculación contractual se establezcan políticas para el uso de medios informáticos, las cuales se den a conocer al trabajador, informando además de los controles que pudiera utilizar el empresario.

En la sentencia 06-10-2010 del Tribunal Supremo se establecen dos consideraciones 1) establecer previamente las reglas de uso de estos medios, con aplicación de prohibiciones absolutas o parciales, 2) informar a los trabajadores de que va a existir un control y las medidas que se aplicarán para garantizar la efectiva utilización laboral del medio.

En caso que los medios se utilicen para usos personales, en contra de las políticas y con conocimiento de los controles no se pueda alegar una violación a la intimidad.

Nos atañe ahora el derecho a garantizar el secreto de las comunicaciones telefónicas y el correo electrónico. Este derecho también cobija a los archivos personales que un trabajador guarde en un ordenador. En el caso en cuestión, los archivos cotejados en la auditoría, corresponden a archivos temporales, denominados cookies, los cuales contienen información de acceso a ciertas páginas de internet, que no contienen información personal, sino información propia de las páginas accesadas, con el fin de no cargar toda la información de la misma en futuros accesos. En la sentencia 03-04-2007 del Tribunal Europeo de Derechos Humanos indica que están incluidos en la protección del artículo 8 del Convenio Europeo de Derechos Humanos "la información derivada del seguimiento del uso personal de Internet", debido a que tales archivos (temporales), pudieran contener información acerca de la ideología, vida sexual, filiación religiosa, etc, del trabajador.

III

De acuerdo a la información suministrada, la prueba fue obtenida a partir de una auditoría informática para revisar la seguridad del sistema y detectar posibles anomalías de utilización de los medios puestos a disposición de los empleados. Así mismo que, la empresa no había definido una política de uso de las nuevas tecnologías puestas a disposición de los trabajadores ni había informado a los trabajadores de que se instauraría un control así como de los medios que se aplicarían en orden a comprobar la corrección del uso de los medios informáticos.

Adicionalmente, en las 66 páginas del "Reporte de Auditoria Detallada del Utilizador", se muestra un estudio de las páginas visitadas y su categorización (motores de búsqueda, música, juegos,

financiero, salud y medicina, redes sociales, etc…), así como un listado de las direcciones visitadas, fecha y hora de acceso, es decir, no es información generalizada sino puntual y particular.

Todo lo anterior lleva a suponer una vulneración al derecho a la intimidad, consagrada en tanto en el artículo 18 de la Constitución Española como en el artículo 8 del Convenio Europeo de Derechos Humanos.